Amendments to the Claims:

Claims 1-40 are currently pending. Claim 1, 19, and 40 have been amended to address minor typographical issues. This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently Amended): A method for validating a restored message, comprising:

generating an entry in a signature log for a message, wherein said entry comprises cryptographic information associated with said message and at least one previous ~~massage~~ message associated with said message;

if said message is lost, generating said restored message responsive to a request; and

validating said restored message using cryptographic information associated with said previous message in said signature log.

2. (Original): The method of claim 1 wherein said signature log comprises a hysteresis signature.

3. (Original): The method of claim 1 wherein said cryptographic information comprises a digital signature.

4. (Original): The method of claim 3 wherein said digital signature is generated using information from a previous signature log entry.

5. (Previously presented): A system for recovering and validating user information, comprising:

a user system comprising a signature log, said signature log comprising cryptographic information associated with said user information and at least one previous version of said user information;

a recovery system coupled with said user system via a communications network for restoring user information; and

a validity system coupled with said user system via said communications network for validating restored user information using said at least one previous version of said user information in said signature log.

6. (Original): The system of claim 5 wherein said user information comprises a log entry of said signature log.

7. (Original): The system of claim 5 wherein said user information comprises a user message.

8. (Original): The system of claim 5 wherein said cryptographic information comprises a hash value.

9. (Original): The system of claim 5 wherein said signature log comprises a first log entry of said signature log determined in part by a second log entry of said signature log.

10. (Previously presented): A system for determining if a user message is valid, said system comprising:

a user computer system having a log, said log comprising a log entry related to a message sent by said user, wherein said log entry has a digital signature comprising information related to a previous log entry of said log; and

a validation unit coupled to said user computer system for validating said user message using said previous log entry of said log.

11. (Original): The system of claim 10 further comprising a collection unit responsive to said validation unit for retrieving said user message, when said user message is lost.

12. (Original): The system of claim 10 further comprising a collection unit responsive to said validation unit for retrieving a copy of said message from a receiver of said message, when said user message is lost.

13. (Original): The system of claim 10 further comprising a publication unit for publishing a selected log entry of said log.

14. (Original): The system of claim 13 wherein said selected log entry is used in validating said user message.

15. (Original): The system of claim 13 wherein publication unit is selected from a group consisting of a newspaper publisher or a Web site.

16. (Original): The system of claim 10 further comprising a notary unit for registering a selected log entry of said log.

17. (Original): The system of claim 10 further comprising a log chain crossing unit coupled to said user computer system and a second user computer system for recording transactions between said user computer system and said second user computer system.

18. (Original): The system of claim 10 further comprising a log chain crossing unit coupled to said user computer system and a second user computer system for facilitating transactions between said user computer system and said second user computer system.

19. (Currently Amended): A computer readable data transmission medium containing a data structure for validating message information comprising:

a first portion having a hash of a user message;

a second portion having a hash of a signature log entry that includes a hash of at least one previous user message that is associated with the user message; and

a digital signature based on said first portion and said second portion.

20. (Original): The computer readable data transmission medium of claim 19 wherein said signature log entry is related to another user message prior to said user message.

21. (Original): The computer readable data transmission medium of claim 19 further comprising a third portion having a timestamp.

22. (Original): A method, using a computer, for generating a signature log comprising a plurality of log entries, said method comprising:

generating a first log entry of said plurality of log entries, said first log entry comprising a first cryptographic value associated with a first user message; and

generating a second log entry of said plurality of log entries, said second log entry comprising a second cryptographic value associated with said first log entry, a third cryptographic value associated with a second user message, and a digital signature.

23. (Original): The method of claim 22 wherein said digital signature is formed using information including said second cryptographic value and said third cryptographic value.

24. (Original): The method of claim 22 wherein said second cryptographic value is a hash of said first log entry.

25. (Original): The method of claim 22 wherein said second log entry further comprises a timestamp.

26. (Original): A data structure stored in a computer readable medium for validating a selected user message of a plurality of user messages, comprising:

a first hash of a first log entry, wherein said first log entry comprises a second hash of a first user message of said plurality of user messages;

a third hash of said selected user message of said plurality of user messages; and

a digital signature of said first hash combined with said third hash.

27. (Previously presented): A computerized method for validating a selected log entry using a signature log having a plurality of recorded log entries, said method comprising:

computing a cryptographic value for said selected log entry; and

determining if said cryptographic value is part of a later recorded log entry of said plurality of recorded log entries.

28. (Original): The method of claim 27 wherein said selected log entry corresponds to a second recorded log entry of said plurality of recorded log entries sequentially prior to said first recorded log entry.

29. (Original): A system for preventing repudiation of a transaction by one of a plurality of user computer systems, said system comprising:

a first user of said plurality of user computer systems;

a second user of said plurality of user computer systems performing said transaction with said first user; and

a log chain crossing computer responsive to a request by either said first or said second user to record said transaction, said record comprising a hysteresis signature of said transaction.

30. (Previously presented): A computerized method for registering a log entry of a user with an officially recognized entity, comprising:

registering a signature log chain with said officially recognized entity, wherein a first log entry of said signature log chain is related to a previous second log entry of said signature log chain;

receiving from said user a user log entry;

generating a cryptographic value associated with said user log entry; and

generating a third log entry in said signature log chain, wherein said third log entry comprises said cryptographic value and cryptographic information for the second log entry and the first log entry.

31. (Original): The method of claim 30 wherein a selected log entry of said signature log chain is published.

32. (Original): The method of claim 30 wherein said officially recognized entity is a notary.

33. (Original): A method for validating a user data item by a computer system using a user's signature log, comprising:

receiving said user's signature log;

validating a cryptographic value associated with said user data item is in a first log entry in said user's signature log;

determining a second log entry in said user's signature log that is checkpointed;

verifying said first log entry by back chaining from said second log entry to said first log entry; and

returning a result to said user.

34. (Previously Presented): A computer method for recovering a data item recorded in a signature log between two points in time, comprising:

receiving a request from a user to recover data recorded in a signature log between two points in time;

receiving from a data recovery unit said data item and a first signature log entry that includes said data item;

receiving from the data recovery unit a second signature log entry entered in the signature log after the first signature log entry is entered in the signature log, wherein the second signature log entry includes another data item associated with said data item;

validating that a hash of said data item is included in said second log entry; and

if said data item is validated, sending said data item to said user.

35. (Previously Presented): A system for validating a user message, comprising:

an input module for receiving a signature log from a user, said signature log comprising a plurality of related log entries;

a cryptographic module for generating a cryptographic value from said user message; and

a verifying module for validating said cryptographic value is in a later log entry in said signature log.

36. (Original): The system of claim 35 further comprising a log verifying module for determining if a first log entry of said plurality of related log entries is compromised, said determining comprising:

selecting a second log entry of said plurality of related log entries subsequent to said first log entry;

hashing said first log entry to give a hash value; and

validating said hash value is part of said second log entry.

37. (Previously presented): A computer program product for validating a restored message, comprising:

code for generating an entry in a signature log for a message, wherein said entry comprises cryptographic information associated with said message and at least one previous massage associated with said message;

when if said message is lost, code for generating said restored message responsive to a request;

code for validating said restored message using cryptographic information associated with said previous message in said signature log; and

a computer usable medium for embodying said codes.

38. (Original): The computer program product of claim 37, wherein said computer usable medium is a storage medium.

39. (Original): The computer program product of claim 37, wherein said computer usable medium is a carrier wave.

40. (Currently Amended): A computer data signal embodied in a carrier wave for validating a restored message, comprising:

program code for generating an entry in a signature log for a message, wherein said entry comprises cryptographic information associated with said message and at least one previous ~~massage~~ message associated with said message;

if said message is lost, program code for generating said restored message responsive to a request; and

program code for validating said restored message using cryptographic information associated with said previous message in said signature log.